to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle C of title VII, add the following:

SEC. 744. LIMITATION ON MEDICAL RESEARCH TO ADDRESS CONDITIONS RELATED TO SERVICE IN THE ARMED FORCES.

Section 2358(c) of title 10, United States Code, is amended—

(1) by striking the period at the end and inserting ''; or'';

(2) by striking ''to finance any research'' and inserting ''to finance—

''(1) any research''; and

(3) by adding at the end the following new paragraph:

''(2) any medical research project unless the project directly addresses treatment of diseases, injuries, or illnesses related to service in the Armed Forces.''.

SA 4108. Mr. LANKFORD submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SECTION _____. EXPEDITED HIRING AUTHORITY.

(a) EXPEDITED HIRING AUTHORITY FOR COLLEGE GRADUATES.—Section 3115(e)(1) of title 5, United States Code, is amended by striking ''15 percent'' and inserting ''25 percent''.

(b) EXPEDITED HIRING AUTHORITY FOR POST-SECONDARY STUDENTS.—Section 3116(d)(1) of title 5, United States Code, is amended by striking ''15 percent'' and inserting ''25 percent''.

SA 4109. Mr. LANKFORD submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. CRITERIA FOR GRANTING DIRECT-HIRE AUTHORITY TO AGENCIES.

Section 3304(a)(3)(B) of title 5, United States Code, is amended by striking ''shortage of candidates'' and all that follows through ''highly qualified candidates)'' and inserting ''shortage of highly qualified candidates''.

SA 4110. Mr. LANKFORD submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. NONCOMPETITIVE ELIGIBILITY FOR HIGH-PERFORMING CIVILIAN EMPLOYEES.

(a) DEFINITIONS.—In this section—

(1) the term ''competitive service'' has the meaning given the term in section 2102 of title 5, United States Code; and

(2) the term ''Executive agency'' has the meaning given the term in section 105 of title 5, United States Code.

(b) REGULATIONS.—Under such regulations as the Director of the Office of Personnel Management shall issue, an Executive agency may noncompetitively appoint, for other than temporary employment, to a position in the competitive service any individual who—

(1) is certified by the Director as having been a high-performing employee in a former position in the competitive service;

(2) has been separated from the former position described in paragraph (1) for less than 6 years; and

(3) is qualified for the new position in the competitive service, as determined by the head of the Executive agency making the noncompetitive appointment.

(c) LIMITATION ON AUTHORITY.—An individual may not be appointed to a position under subsection (b) more than once.

(d) DESIGNATION OF HIGH-PERFORMING EMPLOYEES.—The Director of the Office of Personnel Management shall, in the regulations issued under subsection (b), set forth the criteria for certifying an individual as a ''high-performing employee'' in a former position, which shall be based on—

(1) the final performance appraisal of the individual in that former position; and

(2) a recommendation by the immediate or other supervisor of the individual in that former position.

SA 4111. Mr. LANKFORD submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle D of title X, add the following:

SEC. 1036. REVIEW AND APPROVAL BY SECRETARY OF DEFENSE OF TRANSFER OF DETAINEES FROM UNITED STATES NAVAL STATION, GUANTANAMO BAY, CUBA.

(a) REVIEW AND APPROVAL.—The Secretary of Defense shall review and approve any transfer of an individual detained at Guantanamo from United States Naval Station, Guantanamo Bay, Cuba.

(b) TRANSFER AGREEMENTS.—The Secretary shall sign any agreement relating to the transfer of an individual detained at Guantanamo from United States Naval Station, Guantanamo Bay.

(c) NONDELEGATION.—The Secretary may not delegate any responsibility under subsection (a) or (b).

(d) REPORT REQUIRED.—

(1) IN GENERAL.—During the five-year period beginning on the date on which an individual detained at Guantanamo is transferred from United States Naval Station, Guantanamo Bay, the Secretary shall annually submit to Congress a report on the whereabouts and activities of the individual.

(2) FORM.—Each report required by paragraph (1) shall be submitted in classified form.

(e) INDIVIDUAL DETAINED AT GUANTANAMO DEFINED.—In this section, the term ''individual detained at Guantanamo'' means any individual located at United States Naval Station, Guantanamo Bay, Cuba, as of October 1, 2009, who—

(1) is not a citizen of the United States or a member of the Armed Forces of the United States; and

(2) is—

(A) in the custody or under the control of the Department of Defense; or

(B) otherwise under detention at United States Naval Station, Guantanamo Bay.

SA 4112. Mr. KING (for himself, Mr. ROUNDS, Mr. SASSE, Ms. ROSEN, and Ms. HASSAN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—DEFENSE OF UNITED STATES INFRASTRUCTURE

SEC. 5001. SHORT TITLE.

This division may be cited as the ''Defense of United States Infrastructure Act of 2021''.

SEC. 5002. DEFINITIONS.

In this division:

(1) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such term in section 1016(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

(2) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given such term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

(3) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

TITLE LI—INVESTING IN CYBER RESILIENCY IN CRITICAL INFRASTRUCTURE

SEC. 5101. NATIONAL RISK MANAGEMENT CYCLE.

(a) AMENDMENTS.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2202(c) (6 U.S.C. 652(c))—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in the first paragraph designated as paragraph (12), relating to the Cybersecurity State Coordinator—

(i) by striking ''section 2215'' and inserting ''section 2217''; and

(ii) by striking ''and'' at the end; and

(C) by redesignating the second and third paragraphs designated as paragraph (12) as paragraphs (13) and (14), respectively;

(2) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(3) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(4) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(5) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217;

(6) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216; and

(7) by adding at the end the following:

''SEC. 2220A. NATIONAL RISK MANAGEMENT CYCLE.

''(a) NATIONAL CRITICAL FUNCTIONS DEFINED.—In this section, the term 'national critical functions' means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

''(b) NATIONAL RISK MANAGEMENT CYCLE.—

''(1) RISK IDENTIFICATION AND ASSESSMENT.—

''(A) IN GENERAL.—The Secretary, acting through the Director, shall establish a recurring process by which to identify, assess, and prioritize risks to critical infrastructure, considering both cyber and physical threats, the associated likelihoods, vulnerabilities, and consequences, and the resources necessary to address them.

''(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult with, and request and collect information to support analysis from, Sector Risk Management Agencies, critical infrastructure owners and operators, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the National Cyber Director.

''(C) PUBLICATION.—Not later than 180 days after the date of enactment of this section, the Secretary shall publish in the Federal Register procedures for the process established under subparagraph (A), subject to any redactions the Secretary determines are necessary to protect classified or other sensitive information.

''(D) REPORT.—The Secretary shall submit to the President, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on the risks identified by the process established under subparagraph (A)—

''(i) not later than 1 year after the date of enactment of this section; and

''(ii) not later than 1 year after the date on which the Secretary submits a periodic evaluation described in section 9002(b)(2) of title XC of division H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283).

''(2) NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY.—

''(A) IN GENERAL.—Not later than 1 year after the date on which the Secretary delivers each report required under paragraph (1), the President shall deliver to majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a national critical infrastructure resilience strategy designed to address the risks identified by the Secretary.

''(B) ELEMENTS.—Each strategy delivered under subparagraph (A) shall—

''(i) identify, assess, and prioritize areas of risk to critical infrastructure that would compromise or disrupt national critical functions impacting national security, economic security, or public health and safety;

''(ii) assess the implementation of the previous national critical infrastructure resilience strategy, as applicable;

''(iii) identify and outline current and proposed national-level actions, programs, and efforts to be taken to address the risks identified;

''(iv) identify the Federal departments or agencies responsible for leading each national-level action, program, or effort and the relevant critical infrastructure sectors for each; and

''(v) request any additional authorities necessary to successfully execute the strategy.

''(C) FORM.—Each strategy delivered under subparagraph (A) shall be unclassified, but may contain a classified annex.

''(3) CONGRESSIONAL BRIEFING.—Not later than 1 year after the date on which the President delivers a strategy under this section, and every year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the appropriate committees of Congress on—

''(A) the national risk management cycle activities undertaken pursuant to the strategy; and

''(B) the amounts and timeline for funding that the Secretary has determined would be necessary to address risks and successfully execute the full range of activities proposed by the strategy.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF CONTENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by striking the item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity education and training programs.
''Sec. 2220A. National risk management cycle.''.

(2) ADDITIONAL TECHNICAL AMENDMENT.—

(A) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking ''Homeland Security Act'' and inserting ''Homeland Security Act of 2002''.

(B) EFFECTIVE DATE.—The amendment made by subparagraph (A) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

TITLE LII—IMPROVING THE ABILITY OF THE FEDERAL GOVERNMENT TO ASSIST IN ENHANCING CRITICAL INFRASTRUCTURE CYBER RESILIENCE

SEC. 5201. INSTITUTE A 5-YEAR TERM FOR THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) IN GENERAL.—Subsection (b)(1) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652), is amended by inserting ''The term of office of an individual serving as Director shall be 5 years.'' after ''who shall report to the Secretary.''.

(b) TRANSITION RULES.—The amendment made by subsection (a) shall take effect on the first appointment of an individual to the position of Director of the Cybersecurity and Infrastructure Security Agency, by and with the advice and consent of the Senate, that is made on or after the date of enactment of this Act.

SEC. 5202. PILOT PROGRAM ON CYBER THREAT INFORMATION COLLABORATION ENVIRONMENT.

(a) DEFINITIONS.—In this section:

(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term ''critical infrastructure information'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(2) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(3) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(4) ENVIRONMENT.—The term ''environment'' means the information collaboration environment established under subsection (b).

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''information sharing and analysis organization'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(6) NON-FEDERAL ENTITY.—The term ''non-Federal entity'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(b) PILOT PROGRAM.—The Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General shall carry out a pilot program under which the Secretary shall develop an information collaboration environment and associated analytic tools that enable Federal and non-Federal entities to identify, mitigate, and prevent malicious cyber activity to—

(1) provide limited access to appropriate and operationally relevant data from unclassified and classified intelligence about cybersecurity risks and cybersecurity threats, as well as malware forensics and data from network sensor programs, on a platform that enables query and analysis;

(2) enable cross-correlation of data on cybersecurity risks and cybersecurity threats at the speed and scale necessary for rapid detection and identification;

(3) facilitate a comprehensive understanding of cybersecurity risks and cybersecurity threats; and

(4) facilitate collaborative analysis between the Federal Government and public and private sector critical infrastructure entities and information and analysis organizations.

(c) IMPLEMENTATION OF INFORMATION COLLABORATION ENVIRONMENT.—

(1) EVALUATION.—Not later than 180 days after the date of enactment of this Act, the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in coordination with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General, shall—

(A) identify, inventory, and evaluate existing Federal sources of classified and unclassified information on cybersecurity threats;

(B) evaluate current programs, applications, or platforms intended to detect, identify, analyze, and monitor cybersecurity risks and cybersecurity threats;

(C) consult with public and private sector critical infrastructure entities to identify public and private critical infrastructure cyber threat capabilities, needs, and gaps; and

(D) identify existing tools, capabilities, and systems that may be adapted to achieve the purposes of the environment in order to

maximize return on investment and minimize cost.

(2) IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 1 year after completing the evaluation required under paragraph (1)(B), the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in consultation with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General, shall begin implementation of the environment to enable participants in the environment to develop and run analytic tools referred to in subsection (b) on specified data sets for the purpose of identifying, mitigating, and preventing malicious cyber activity that is a threat to public and private critical infrastructure.

(B) REQUIREMENTS.—The environment and the use of analytic tools referred to in subsection (b) shall—

(i) operate in a manner consistent with relevant privacy, civil rights, and civil liberties policies and protections, including such policies and protections established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

(ii) account for appropriate data standards and interoperability requirements, consistent with the standards set forth in subsection (d);

(iii) enable integration of current applications, platforms, data, and information, including classified information, in a manner that supports integration of unclassified and classified information on cybersecurity risks and cybersecurity threats;

(iv) incorporate tools to manage access to classified and unclassified data, as appropriate;

(v) ensure accessibility by entities the Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General, determines appropriate;

(vi) allow for access by critical infrastructure stakeholders and other private sector partners, at the discretion of the Secretary, in consultation with the Secretary of Defense;

(vii) deploy analytic tools across classification levels to leverage all relevant data sets, as appropriate;

(viii) identify tools and analytical software that can be applied and shared to manipulate, transform, and display data and other identified needs; and

(ix) anticipate the integration of new technologies and data streams, including data from government-sponsored network sensors or network-monitoring programs deployed in support of non-Federal entities.

(3) ANNUAL REPORT REQUIREMENT ON THE IMPLEMENTATION, EXECUTION, AND EFFECTIVENESS OF THE PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, and every year thereafter until the date that is 1 year after the pilot program under this section terminates under subsection (e), the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, and the Permanent Select Committee on Intelligence of the House of Representatives a report that details—

(A) Federal Government participation in the environment, including the Federal entities participating in the environment and the volume of information shared by Federal entities into the environment;

(B) non-Federal entities' participation in the environment, including the non-Federal entities participating in the environment and the volume of information shared by non-Federal entities into the environment;

(C) the impact of the environment on positive security outcomes in the Federal Government and non-Federal entities;

(D) barriers identified to fully realizing the benefit of the environment both for the Federal Government and non-Federal entities; and

(E) additional authorities or resources necessary to successfully execute the environment.

(d) CYBER THREAT DATA STANDARDS AND INTEROPERABILITY.—

(1) ESTABLISHMENT.—The Secretary, in coordination with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General, shall establish data standards and requirements for non-Federal entities to participate in the environment.

(2) DATA STREAMS.—The Secretary shall identify, designate, and periodically update programs that shall participate in or be interoperable with the environment, which may include—

(A) network-monitoring and intrusion detection programs;

(B) cyber threat indicator sharing programs;

(C) certain government-sponsored network sensors or network-monitoring programs;

(D) incident response and cybersecurity technical assistance programs; or

(E) malware forensics and reverse-engineering programs.

(3) DATA GOVERNANCE.—The Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, the Director of the National Security Agency, and the Attorney General shall establish procedures and data governance structures, as necessary, to protect sensitive data, comply with Federal regulations and statutes, and respect existing consent agreements with public and private sector critical infrastructure entities that apply to critical infrastructure information.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall change existing ownership or protection of, or policies and processes for access to, agency data.

(e) DURATION.—The pilot program under this section shall terminate on the date that is 5 years after the date of enactment of this Act.

TITLE LIII—IMPROVING SECURITY IN THE NATIONAL CYBER ECOSYSTEM

SEC. 5301. REPORT ON CYBERSECURITY CERTIFICATIONS AND LABELING.

Not later than October 1, 2022, the National Cyber Director, in consultation with the Director of the National Institute of Standards and Technology and the Director of the Cybersecurity and Infrastructure Security Agency, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that—

(1) identifies and assesses existing efforts by the Federal Government to create, administer, or otherwise support the use of certifications or labels to communicate the security or security characteristics of information technology or operational technology products and services; and

(2) assesses the viability of and need for a new program at the Department to harmonize information technology and operational technology product and service security certification and labeling efforts across the Federal Government and between the Federal Government and the private sector.

SEC. 5302. SECURE FOUNDATIONAL INTERNET PROTOCOLS.

(a) DEFINITIONS.—In this section:

(1) BORDER GATEWAY PROTOCOL.—The term ''border gateway protocol'' means a protocol designed to optimize routing of information exchanged through the internet.

(2) DOMAIN NAME SYSTEM.—The term ''domain name system'' means a system that stores information associated with domain names in a distributed database on networks.

(3) INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE PROVIDERS.—The term ''information and communications technology infrastructure providers'' means all systems that enable connectivity and operability of internet service, backbone, cloud, web hosting, content delivery, domain name system, and software-defined networks and other systems and services.

(b) CREATION OF A STRATEGY TO ENCOURAGE IMPLEMENTATION OF MEASURES TO SECURE FOUNDATIONAL INTERNET PROTOCOLS.—

(1) PROTOCOL SECURITY STRATEGY.—In order to encourage implementation of measures to secure foundational internet protocols by information and communications technology infrastructure providers, not later than 180 days after the date of enactment of this Act, the Assistant Secretary for Communications and Information of the Department of Commerce, in coordination with the Director of the National Institute Standards and Technology and the Director of the Cybersecurity and Infrastructure Security Agency, shall establish a working group composed of appropriate stakeholders, including representatives of the Internet Engineering Task Force and information and communications technology infrastructure providers, to prepare and submit to Congress a strategy to encourage implementation of measures to secure the border gateway protocol and the domain name system.

(2) STRATEGY REQUIREMENTS.—The strategy required under paragraph (1) shall—

(A) articulate the motivation and goal of the strategy to reduce incidents of border gateway protocol hijacking and domain name system hijacking;

(B) articulate the security and privacy benefits of implementing the most up-to-date and secure instances of the border gateway protocol and the domain name system and the burdens of implementation and the entities on whom those burdens will most likely fall;

(C) identify key United States and international stakeholders;

(D) outline varying measures that could be used to implement security or provide authentication for the border gateway protocol and the domain name system;

(E) identify any barriers to implementing security for the border gateway protocol and the domain name system at scale;

(F) propose a strategy to implement identified security measures at scale, accounting for barriers to implementation and balancing benefits and burdens, where feasible; and

(G) provide an initial estimate of the total cost to the Government and implementing entities in the private sector of implementing security for the border gateway protocol and the domain name system and propose recommendations for defraying these costs, if applicable.

TITLE LIV—ENABLING THE NATIONAL CYBER DIRECTOR

SEC. 5401. ESTABLISHMENT OF HIRING AUTHORITIES FOR THE OFFICE OF THE NATIONAL CYBER DIRECTOR.

(a) DEFINITIONS.—In this section—

(1) the term ''Director'' means the National Cyber Director;

(2) the term ''excepted service'' has the meaning given such term in section 2103 of title 5, United States Code;

(3) the term ''Office'' means the Office of the National Cyber Director;

(4) the term ''qualified position'' means a position identified by the Director under subsection (b)(1)(A), in which the individual occupying such position performs, manages, or supervises functions that execute the responsibilities of the Office.

(b) HIRING PLAN.—The Director shall, for purposes of carrying out the functions of the Office—

(1) craft an implementation plan for positions in the excepted service in the Office, which shall propose—

(A) qualified positions in the Office, as the Director determines necessary to carry out the responsibilities of the Office; and

(B) subject to the requirements of paragraph (2), rates of compensation for an individual serving in a qualified position;

(2) propose rates of basic pay for qualified positions, which shall—

(A) be determined in relation to the rates of pay provided for employees in comparable positions in the Office, in which the employee occupying the comparable position performs, manages, or supervises functions that execute the mission of the Office; and

(B) subject to the same limitations on maximum rates of pay and consistent with section 5341 of title 5, United States Code, adopt such provisions of that title to provide for prevailing rate systems of basic pay and apply those provisions to qualified positions for employees in or under which the Office may employ individuals described by section 5342(a)(2)(A) of such title; and

(3) craft proposals to provide—

(A) employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5, United States Code; and

(B) employees in a qualified position for which the Director proposes a rate of basic pay under paragraph (2) an allowance under section 5941 of title 5, United States Code, on the same basis and to the same extent as if the employee was an employee covered by such section, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

SA 4113. Mr. MANCHIN (for himself, Mr. LUJÁN, and Mrs. CAPITO) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. AMOUNTS FOR NEXT GENERATION RADAR AND RADIO ASTRONOMY IMPROVEMENTS AND RELATED ACTIVITIES.

(a) IN GENERAL.—There are authorized to be appropriated to the National Science Foundation, $176,000,000 for the period of fiscal years 2022 through 2024 for the design, development, prototyping, or mid-scale upgrades of next generation radar and radio astronomy improvements and related activities under section 14 of the National Science Foundation Authorization Act of 2002 (42 U.S.C. 1862n-4).

(b) APPROVAL.—Nothing in this section shall amend the Director of the National Science Foundation's authority to review and issue awards.

SA 4114. Mr. MANCHIN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. EXPANSION OF APPALACHIAN DEVELOPMENT HIGHWAY SYSTEM.

Section 14501 of title 40, United States Code, is amended—

(1) in subsection (a), in the second sentence, by striking ''three thousand and ninety miles'' and inserting ''the total number of miles established by the Secretary under subsection (h)''; and

(2) by adding at the end the following:

''(h) EXPANSION OF THE APPALACHIAN DEVELOPMENT HIGHWAY SYSTEM.—As soon as practicable after the date of enactment of this subsection, the Secretary shall establish the total number of miles that is authorized to be constructed for the Appalachian development highway system under subsection (a) based on—

''(1) a report prepared by the Secretary before the date of enactment of this subsection in which the Secretary describes the total number of miles that should be authorized to be constructed for the Appalachian development highway system under subsection (a); or

''(2) if the Secretary determines that there is not an existing report that addresses the matters described in paragraph (1), a report prepared by the Secretary, in consultation with the Appalachian Regional Commission and applicable State departments of transportation, as soon as practicable after the date of enactment of this subsection, that describes the total number of miles that should be authorized to be constructed for the Appalachian development highway system under subsection (a).''.

SA 4115. Mr. MANCHIN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. OPIOID SUBSTANCE ABUSE REDUCTION.

(a) STEWARDSHIP FEE ON OPIOID PAIN RELIEVERS.—

(1) IN GENERAL.—Chapter 32 of the Internal Revenue Code of 1986 is amended by inserting after subchapter D the following new subchapter:

''Subchapter E—Certain Opioid Pain Relievers

''Sec. 4191. Opioid pain relievers.

''SEC. 4191. OPIOID PAIN RELIEVERS.

''(a) IN GENERAL.—There is hereby imposed on the sale of any active opioid by the manufacturer, producer, or importer a fee equal to 1 cent per milligram so sold.

''(b) ACTIVE OPIOID.—For purposes of this section—

''(1) IN GENERAL.—The term 'active opioid' means any controlled substance (as defined in section 102 of the Controlled Substances Act, as in effect on the date of the enactment of this section) which is opium, an opiate, or any derivative thereof.

''(2) EXCLUSION FOR CERTAIN PRESCRIPTION MEDICATIONS.—Such term shall not include any prescribed drug which is used exclusively for the treatment of opioid addiction as part of a medically assisted treatment effort.

''(3) EXCLUSION OF OTHER INGREDIENTS.—In the case of a product that includes an active opioid and another ingredient, subsection (a) shall apply only to the portion of such product that is an active opioid.

''(c) REBATE OR DISCOUNT PROGRAM FOR CERTAIN CANCER AND HOSPICE PATIENTS.—

''(1) IN GENERAL.—The Secretary of Health and Human Services, in consultation with patient advocacy groups and other relevant stakeholders as determined by such Secretary, shall establish a mechanism by which—

''(A) any amount paid by an eligible patient in connection with the stewardship fee under subsection (a) shall be rebated to such patient in as timely a manner as possible, or

''(B) amounts paid by an eligible patient for active opioids are discounted at time of payment or purchase to ensure that such patient does not pay any amount attributable to such fee,

with as little burden on the patient as possible. The Secretary of Health and Human Services shall choose whichever of the options described in subparagraph (A) or (B) is, in such Secretary's determination, most effective and efficient in ensuring eligible patients face no economic burden from such fee.

''(2) ELIGIBLE PATIENT.—For purposes of this subsection, the term 'eligible patient' means—

''(A) a patient for whom any active opioid is prescribed to treat pain relating to cancer or cancer treatment,

''(B) a patient participating in hospice care,

''(C) a patient with respect to whom the prescriber of the applicable opioid determines that other non-opioid pain management treatments are inadequate or inappropriate, and

''(D) in the case of the death or incapacity of a patient described in subparagraph (A), (B), or (C), or any similar situation as determined by the Secretary of Health and Human Services, the appropriate family member, medical proxy, or similar representative or the estate of such patient.''.

(2) CLERICAL AMENDMENT.—The table of subchapters for chapter 32 of the Internal Revenue Code of 1986 is amended by inserting after the item relating to subchapter D the following new item:

''SUBCHAPTER E. CERTAIN OPIOID PAIN RELIEVERS''.

(3) EFFECTIVE DATE.—The amendments made by this subsection shall apply to sales on or after the later of—

(A) the date which is 1 year after the date of the enactment of this Act; or

(B) the date on which the Secretary of Health and Human Services establishes the mechanism described in subsection (c)(1) of section 4191 of the Internal Revenue Code of 1986, as added by this section.

(b) BLOCK GRANTS FOR PREVENTION AND TREATMENT OF SUBSTANCE ABUSE.—

(1) GRANTS TO STATES.—Section 1921(b) of the Public Health Service Act (42 U.S.C.